IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Docket No.: **TI-34921**
Eric Balard	Examiner: **Lanier, Benjamin E.**
Serial No.: **10/618,861**	Art Unit: **2132**
Filed: **07/14/2003**	Conf. No.: **6971**

For: **SECURE PROTECTION METHOD FOR ACCESS TO PROTECTED RESOURCES IN A PROCESSOR**

APPELLANTS' BRIEF – 37 C.F.R. § 1.192(c)

Commissioner for Patents

P.O. Box 1450

Alexandria, VA 22313-1450

Dear Sir:

This Appeal Brief is submitted in connection with the above-identified application in response to the final Office Action dated November 1, 2007 mailed November 1, 2007.

I. REAL PARTY IN INTEREST

Texas Instruments Incorporated is the real party in interest.

II. RELATED APPEALS AND INTERFERENCES

Appellants are not aware of pending appeals in any related applications.

III. STATUS OF CLAIMS

Claims 1-46 are pending in the application. A final rejection of Claims 1-46 was made by the Examiner in an Office Action dated November 1, 2007 dated November 1, 2007. Appellants hereby appeal the rejection of Claims 1-46. Claims 1-46 are on appeal. Claims 1-46 are reproduced in the Appendix to Appellants' Brief filed herewith.

IV. STATUS OF AMENDMENTS

Appellant submitted an Amendment under 37 CFR 1.116 on March 11, 2008, requesting reconsideration of the Final rejection dated November 1, 2007. In an Advisory action dated March 28, 2008, Examiner refused to enter the amendment. Appellants will submit on the same date as this Appeal Brief an Amendment under 37 CFR 1.116. No amendment to the claims is being made thus Appellants anticipate the Amendment will be entered.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

Access to resources in a computing device is secured by storing an encrypted access code in a known memory location within the computing device. A password to access the resources is received in the computing device and the password is encrypted to produce an encrypted password. The encrypted password is compared to the encrypted access code and access to the resources is allowed only if the encrypted access code matches the encrypted password. More particularly:

Claim 1 requires and positively recites, a method of securing access to resources in a computing device (10),comprising the steps of: "storing an encrypted access code

((H_Man_Pub_Key) page 11, lines 3-15; (H_Test_Id) page 11, lines 12-15 & page 30, lines 8-11) in a memory location within the computing device", "receiving a password to access the resources ((Man_Pub_Key) Figure 4; ((Input_Test_ID) page 30, lines 11-12)", "encrypting the password to produce a encrypted password ((SHA-1 Hashing) Figure 4; page 30, line 12)", "comparing the encrypted password to the encrypted access code ((COMPARE) Figure 4; page 30, lines 12-13)" and "allowing access to the resources if the encrypted access code matches the encrypted password ((MATCH) Figure 4; (page 30, lines 13-14)".

Claim 7 requires and positively recites, a computing device ((10) Figure 1, page 7, line 10) comprising: "a processing system ((12) Figure 1, page 7, line11)", "a memory ((18/24) Figure 1, page 7, lines 14-16) coupled to the processing system for storing an encrypted access code", "input circuitry ((28) Figure 1, page 7, lines 18-20) coupled to the processing system for receiving a password to access resources; and "wherein the processing circuitry: encrypts the password to produce a encrypted password ((SHA-1 Hashing) Figure 4; page 30, line 12); compares the encrypted password to the encrypted access code ((COMPARE) Figure 4; page 30, lines 12-13); allows access to the resources if the encrypted access code matches the encrypted password ((MATCH) Figure 4; (page 30, lines 13-14)".

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1) Are Claims 1, 4-7 and 10-13, 15-21, 23-24, 26-28, 30, 33-38, 40, 41 and 43-45 patentable under 35 U.S.C. 102(e) over Gray, US patent, 6,268,788?

2) Are Claims 2, 3, 8, 9, 29 and 46 patentable under 35 U.S.C. 103(a) over Gray and Lohstroh et al, US patent 5,768,373?

3) Are Claims 14, 25, 31, 32 and 42 patentable under 35 U.S.C. 103(a) over Gray in

view of Reddy, US patent 6,824,051?

4) Are Claims 22 and 39 patentable under 35 U.S.C. 103(a) over Gray in view of Debry, US patent 6,341,521?

VII. ARGUMENTS

1) Claims 1, 4-7 and 10-13, 15-21, 23-24, 26-28, 30, 33-38, 40, 41 and 43-45 stand rejected under 35 U.S.C. 102(e) as being anticipated by Gray, US patent, 6,268,788. Appellants respectfully traverse this rejection as set forth:

In order that the rejection of Claims 1, 4-7 and 10-13, 15-21, 23-24, 26-28, 30, 33-38, 40, 41 and 43-45 be sustainable, it is fundamental that "each and every element as set forth in the claims be found, either expressly or inherently described, in a single prior art reference." Verdegall Bros. v. Union Oil Co. of California, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). See also, Richardson v. Suzuki Motor Co., 9 USPQ2d 1913, 1920 (Fed. Cir. 1989), where the court states, "The identical invention must be shown in as complete detail as is contained in the ... claim".

Furthermore, "all words in a claim must be considered in judging the patentability of that claim against the prior art." In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

Independent Claim 1, as amended, requires and positively recites, a method of **securing access to resources in a computing device**, comprising the steps of: "storing an encrypted access code **in a memory location within the computing device**", "receiving a password **to access the resources**", "encrypting the password to produce a encrypted password", "comparing

the encrypted password to the encrypted access code", and "**allowing access to the resources** if the encrypted access code matches the encrypted password".

Independent Claim 7, as amended, requires and positively recites, **a computing device** comprising: "a processing system", "a **memory coupled to the processing system for storing an encrypted access code**", "input circuitry coupled to the processing system for receiving a password to **access resources**, wherein the processing circuitry: encrypts the password to produce a encrypted password; compares the encrypted password to the encrypted access code; and allows access to the resources if the encrypted access code matches the encrypted password".

In the Office Action dated November 1, 2007 dated November 1, 2007, Examiner admits that Gray's verification unit 20 is not part of computer 12, being that verification unit 20 is externally interposed between keyboard 16 and computer 12 (see Figs. 1, 2; col. 4, lines 13-20)(Office Action dated November 1, 2007 page 2, lines 3-5). Examiner, however, now equates Gray's verification unit 20 with "computing device" of Claims 1 and 7 and maintains the 35 U.S.C. 102(e) rejection of independent Claims 1 and 7. Appellants respectfully traverse the rejection as set forth below.

To the extent verification unit 20 has memory, it is not used to store any access code (much less an encrypted access code). Gray specifically teaches that verification data such as a security identification number, a password, or a Personal Identification Number (PIN) of the operation requesteding control of the application software is stored on card 34 (col. 4, lines 36-39) – NOT within memory within verification unit 20. Moreover, it is the card 34 that issues a "pass" or a "fail" signal via verification unit 20 to the computer 12, which either grants or denies execution control of application software to the operation (col. 4, lines 40-43). Accordingly, Gray fails to teach or suggest, "storing an encrypted access code **in a memory location within**

the computing device", as required by Claim 1, OR a **computing device comprising**, "a **memory coupled to the processing system for storing an encrypted access code**", as required by Claim 7. For this reason alone, the 35 U.S.C. 102(e) rejection of Claims 1 and 7 is improper is improper and must be reversed since each and every element of the claims is not contained in the Gray reference.

Examiner counters and argues that "card 34" is a smartcard and has its own memory. Therefore, according to Examiner, the smartcard itself is a memory within the verification unit 20 (Office Action dated November 1, 2007, page 2, lines 15-18). Examiner goes on to argue that the encrypted password stored in the smart card is additionally stored in the RAM 66 of the verification unit 20 prior to comparison with the entered password – therefore Gray meets the claim limitation for at least two different reasons (Office Action dated November 1, 2007, page 2, line 18 – page 3, line 2). Appellants respectfully counter that card 34 is a peripheral device that is NOT part of verification unit 20. Card 34 is a mobile device that can be coupled to verification unit 20 when inserted into card reader/writer 68. Card 34 is no more a part of verification unit 20 than keyboard 16 or any other device that is coupled to verification unit 20 via an external connection means. Accordingly, Examiner's determination seems to be supposition not supported by fact.

Even if, arguendo, Examiner's determination that Card 34 is physically part of verification unit 20 were correct, verification unit 20 does not authorize access to resources within verification unit 20 – it only compares passwords, with card 34 issuing a "pass" or a "fail" signal via the verification unit 20 to the computer 12, which either grants or denies execution control of application software to the operator (Col. 4, lines 36-43). Accordingly, verification unit 20 fails to teach or suggest, "input circuitry coupled to the processing system for receiving a password to **access resources in the computing device"** (computing device in this case being

verification unit 20 – no password matching is required to access resources within verification unit 20), as required by Claims 1 and 7.

In light of the above, it should be clear that that each and every element of Claims 1 and 7 are NOT found expressly, or inherently, in the Gray reference. See, *Verdegall Bros. v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). See also, *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989)". Accordingly, the 35 U.S.C. 102(e) rejection of Claims 1 and 7 is improper and must be reversed.

Claims 4-6, 13, 15-21, 23, 24 and 26-28 stand allowable as depending directly or indirectly from allowable Claim 1 and Claims 10-12, 30, 33-38, 40-41 and 43-45 stand allowable as depending directly from allowable Claim 7 and by including further limitations not taught or suggested by the reference of record.

Claim 4 further defines the method of claim 1 wherein the encrypted access code is stored in **a memory that cannot be externally modified**. Claim 4 depends from Claim 1 and is therefore allowable for the same reasons set forth above for the allowance of Claim 1. Moreover, and contrary to Examiner's determination, Gray does not teach (Col. 5, line 62- Col. 6, line 20) & (Col. 9, lines 53-65) that its memories CANNOT be externally modified. Gray specifically teaches that the encrypted password is read from card 34 and stored in RAM 66 (Col. 6, lines 57-60). Accordingly, Examiner's determination is supposition not supported by fact. Appellants requesteded Examiner to specifically identify the memory in Gray that CANNOT be externally modified and identify the text supporting such determination or withdraw the rejection (Amendment dated March 11, 2008, page 18, lines 14-16) – Examiner did not respond.

Claim 5 further defines the method of claim 1 wherein the step of allowing access comprises the step of **allowing access to testing resources if the encrypted access code matches the encrypted password**. Claim 5 depends from Claim 1 and is therefore allowable for the same reasons set forth above for the allowance of Claim 1. Moreover, contrary to Examiner's determination, nothing in Gray (Col. 6, lines 55 – Col. 7, line 10) teaches or suggests "**allowing access to testing resources if the encrypted access code matches the encrypted password**". Examiner's determination is supposition not supported by fact. Appellants requested Examiner to specifically identify the testing resources in Gray that are made accessible to a user if the encrypted access code matches the encrypted password or withdraw the rejection (Amendment dated March 11, 2008, page 18, line 24 – page 19, line 2) – Examiner did not respond.

Claim 6 further defines the method of claim 1 wherein the step of allowing access comprises the step of **allowing access to change system parameters if** the encrypted access code matches the encrypted password. Claim 6 depends from Claim 1 and is therefore allowable for the same reasons set forth above for the allowance of Claim 6. Moreover, while an operator may access and/or alter the application program(s) unlocked through use of the password, (Col. 7, lines 5-7), Gray does not teach or suggest that a user will be able to change system parameters, as suggested by Examiner. Accordingly, Examiner's determination is supposition not supported by fact. Appellants requesteded Examiner to specifically identify the testing resources in Gray that are made accessible to a user if the encrypted access code matches the encrypted password or withdraw the rejection (Amendment dated March 11, 2008, page 19, lines 10-13) – Examiner did not respond.

Claim13 further defines the method of claim 1 wherein the **memory location is within a processing system in the computing device**. Claim 13 depends from Claim 1 and is therefore allowable for the same reasons set forth above for the allowance of Claim 1. Moreover, Gray

clearly shows in Fig. 2 that ROM 64 and RAM 66 5, are part of a memory module 62, which is separate from processor 60 (Col. 5, lines 31-34) – not part of processor 60.

Appellants further traverse Examiner's determination that "it is clear that the computer 12 and the verification unit 20 make up a singular device for the simple reason that "the verification units 20 draws its power from the computer 12, which meets the limitation of the memory location is within a processing system in the computing device". In reality computer 12 does not need verification unit 20 to operate. Whether or not the reverse is true is irrelevant. Keyboard 16 also draws its power from computer 12 (Col. 4, lines 18-20). Using Examiner's reasoning, keyboard 16 would also be defined as part of "the processing system", which it is not. Keyboard 16 similarly has no function without being hooked up to computer 12. But the same could be said about other peripherals (such as floppy drives, CD ROM drives, DVD players, memory sticks, etc, that derive their power from a computer to which they are coupled. Certainly Examiner would not consider them mandatory parts of the processing system? Accordingly, Appellants requested Examiner to cite authority for his determination or withdraw the rejection (Amendment dated March 11, 2008, page 20, lines 6-8) – Examiner did not respond.

Claim 15 further defines the method of claim 13 wherein the memory location **is in a memory subsystem within the processing system**. Claim 15 depends from Claim 13 and is therefore allowable for the same reasons set forth above for the allowance of Claim 13. Moreover, Gray clearly shows in Fig. 2 that ROM 64 and RAM 66 5, are part of a memory module 62, which is separate from processor 60 (Col. 5, lines 31-34) – not part of processor 60.

Appellants further traverse Examiner's determination that "it is clear that the computer 12 and the verification unit 20 make up a singular device for the simple reason that "the verification units 20 draws its power from the computer 12, which meets the limitation of the memory location is within a processing system in the computing device". In reality computer 12 does not need verification unit 20 to operate. Whether or not the reverse is true is irrelevant. Keyboard

16 also draws its power from computer 12 (Col. 4, lines 18-20). Using Examiner's reasoning, keyboard 16 would also be defined as part of "the processing system", which it is not. Keyboard 16 similarly has no function without being hooked up to computer 12. But the same could be said about other peripherals (such as floppy drives, CD ROM drives, DVD players, memory sticks, etc, that derive their power from a computer to which they are coupled. Certainly Examiner would not consider them mandatory parts of the processing system? Accordingly, Appellants requested Examiner to cite authority for his determination or withdraw the rejection (Amendment dated March 11, 2008, page 21, lines 1-2) – Examiner did not respond.

Claim 16 further defines the method of claim 15 wherein the memory subsystem comprises **a memory array in which after data is written to the array, further writing to the particular memory location is disabled, such that the data cannot be overwritten**. Claim 16 depends from Claim 15 and is therefore allowable for the same reasons set forth above for the allowance of Claim 15.

Gray, on the other hand, includes both ROM 64 and RAM 66 in its memory module 62. While it may not be possible to write to ROM 64 it would be possible to write to RAM 66.

Claim 17 further defines the method of claim 16 by further including **at least one of a read only memory (ROM) coupled to the memory array and a random access memory (RAM) coupled to the memory array**. Claim 17 depends from Claim 16 and is therefore allowable for the same reasons set forth above for the allowance of Claim 16. Moreover, in Gray, ROM 64 and RAM 66 are the memory array in verification unit 20 – they are not "coupled to a memory array".

Claim 18 further defines the method of claim 16 wherein some portions of the memory array are externally accessible but not modifiable. Claim 18 depends from Claim 16 and is therefore allowable for the same reasons set forth above for the allowance of Claim 16.

Claim 19 further defines the method of claim 16 wherein **some portions of the memory array are not externally accessible and are not modifiable**. Claim 19 depends from Claim 16 and is therefore allowable for the same reasons set forth above for the allowance of Claim 16. Examiner points out that Gray teaches that memory can be password protected (Col. 9, lines 21-28)(Office Action dated November 1, 2007, page 8, lines 5-7). But Appellants respond that Examiner's above determination is an admission that someone with the password WOULD HAVE ACCESS to the memory – thus Gray fails to teach or suggest, "wherein **some portions of the memory array are not externally accessible and are not modifiable**", as required by Claim 19. Accordingly, the rejection is improper and must be reversed.

Claim 20 further defines the method of claim 16 wherein an encryption key is **stored in the memory array**. Claim 20 depends from Claim 16 and is therefore allowable for the same reasons set forth above for the allowance of Claim 16. Moreover, the encryption key in stored in memory on card 34. When the encryption key is read into memory module 62, it is read into RAM 66. Thus, when the encryption key is the data being read into the memory module, it can not be equated to **a memory array in which after data is written to the array, further writing to the particular memory location is disabled, such that the data cannot be overwritten**, as required by Claim 16, the claim upon which Claim 20 depends.

Claim 21 further defines the method of claim 20 wherein **the encryption key is generated by a random number generator internal to the processing system**. Claim 21 depends from Claim 20 and is therefore allowable for the same reasons set forth above for the allowance of Claim 20. Moreover, the extent Gray's verification unit does generates something, it generates "session keys" that are sent to the PACS residing the CPU 40 for using in preparing classified documents and files (Col. 12, lines 8-10). Verification unit 20 may "manage" cipher keys that protect other keys (Col. 12, lines 6-7), but it does not "generate" the encryption keys. Encryption keys are transferred from cards 34 and then stored in RAM 66 for comparison to the

keys being input via keyboard 16 – NOT "**generated by a random number generator internal to the processing system**", as required by Claim 21.

Claim 23 further defines the method of claim 15, further including at least one processor coupled to the memory subsystem. Claim 23 depends from Claim 15 and is therefore allowable for the same reasons set forth above for the allowance of Claim 15.

Claim 24 further defines the method of claim 23, further including a non-volatile memory system coupled to the processing system wherein the non-volatile memory system is external to the processing system but internal to the computing device. Claim 24 depends from Claim 23 and is therefore allowable for the same reasons set forth above for the allowance of Claim 23. In addition to the above, if Examiner takes the position that Gray's memory module 62 and processor 60 are the "processing system", then Gray further fails to teach or suggest, "a non-volatile memory system coupled to the processing system wherein **the non-volatile memory system is external to the processing system but internal to the computing device**".

Claim 26 further defines the method of claim 16, further comprising **at least one of the following stored in the array: a test ID; a manufacturer's public key; a die identification number**. Claim 26 depends from Claim 16 and is therefore allowable for the same reasons set forth above for the allowance of Claim 16. Moreover, in Gray, upon receipt of the password from keyboard 16, verification unit 20 encrypts and temporarily stores the password in RAM 66 (Col. 6, lines 55-57). It then proceeds to read the encrypted password stored into the in the card 34 through card reader 68, and compares the encrypted password received from the card 34 with the encrypted password stored in RAM 66 (Col. 6, lines 57-60). Gray, however, fails to further teach or suggest, "**at least one of the following stored in the array: a test ID; a manufacturer's public key; a die identification number**", as further required by Claim 26.

Claim 27 further defines the method of claim 17 wherein the read only memory (ROM) further comprises at least one of the following: a program for determining whether boot system firmware is available for uploading at power-up; a program for checking authenticity and integrity of the system boot firmware; a program for preventing alternation of specific data associated with the computing device; a program for preventing alteration or swapping of firmware; cryptographic software. Claim 27 depends from Claim 17 and is therefore allowable for the same reasons set forth above for the allowance of Claim 17.

Claim 28 further defines the method of claim 24, wherein the non-volatile memory system includes at least one of the following: firmware; application software; data files; a manufacturer's certificate; a platform certificate. Claim 28 depends from Claim 24 and is therefore allowable for the same reasons set forth above for the allowance of Claim 24.

Claim 10 further defines the computing device of claim 7 wherein the encrypted access code is stored in **a memory that cannot be externally modified**. Claim 10 depends from Claim 7 and is therefore allowable for the same reasons set forth above for the allowance of Claim 7. Moreover, and contrary to Examiner's determination, Gray does not teach (Col. 5, line 62- Col. 6, line 20) & (Col. 9, lines 53-65) that its memories CANNOT be externally modified. Gray specifically teaches that the encrypted password is read from card 34 and stored in RAM 66 (Col. 6, lines 57-60). Accordingly, Examiner's determination is supposition not supported by fact. Appellants requested Examiner to specifically identify the memory in Gray that CANNOT be externally modified and identify the text supporting such determination or withdraw the rejection (Amendment dated March 11, 2008, page 24, lines 21-23) – Examiner did not respond.

Claim 11 further defines the computing device of claim 7 wherein the processing system **allows access to testing resources if the encrypted access code matches the encrypted password**. Claim 11 depends from Claim 7 and is therefore allowable for the same reasons set forth above for the allowance of Claim 7. Moreover, contrary to Examiner's determination,

nothing in Gray (Col. 6, lines 55 – Col. 7, line 10) teaches or suggests "**allowing access to testing resources if the encrypted access code matches the encrypted password**". Examiner's determination is supposition not supported by fact. Appellants requested Examiner to specifically identify the testing resources in Gray that are made accessible to a user if the encrypted access code matches the encrypted password or withdraw the rejection (Amendment dated March 11, 2008, page 25, lines 8-10) – Examiner did not respond.

Claim 12 further defines the computing device of claim 7 wherein the processing system **allows access to system parameters** if the encrypted access code matches the encrypted password. Claim 12 depends from Claim 7 and is therefore allowable for the same reasons set forth above for the allowance of Claim 7. Moreover, while an operator may access and/or alter the application program(s) unlocked through use of the password, (Col. 7, lines 5-7), Gray does not teach or suggest that a user will be able to change system parameters, as suggested by Examiner. Accordingly, Examiner's determination is supposition not supported by fact. Appellants requested Examiner to specifically identify the testing resources in Gray that are made accessible to a user if the encrypted access code matches the encrypted password or withdraw the rejection (Amendment dated March 11, 2008, page 25, lines 18-20) – Examiner did not respond.

Claim 30 further defines the computing device of claim 7 wherein the memory is **a memory subsystem within the computing device**. Claim 30 depends from Claim 7 and is therefore allowable for the same reasons set forth above for the allowance of Claim 7. Moreover, Gray clearly shows in Fig. 2 that ROM 64 and RAM 66 5, are part of a memory module 62, which is separate from processor 60 (Col. 5, lines 31-34) – not part of processor 60.

Appellants further traverse Examiner's determination that "it is clear that the computer 12 and the verification unit 20 make up a singular device for the simple reason that "the verification units 20 draws its power from the computer 12, which meets the limitation of the memory

location is within a processing system in the computing device". In reality computer 12 does not need verification unit 20 to operate. Whether or not the reverse is true is irrelevant. Keyboard 16 also draws its power from computer 12 (Col. 4, lines 18-20). Using Examiner's reasoning, keyboard 16 would also be defined as part of "the processing system", which it is not. Keyboard 16 similarly has no function without being hooked up to computer 12. But the same could be said about other peripherals (such as floppy drives, CD ROM drives, DVD players, memory sticks, etc, that derive their power from a computer to which they are coupled. Certainly Examiner would not consider them mandatory parts of the processing system? Accordingly, Appellants requested Examiner to cite authority for his determination or withdraw the rejection (Amendment dated March 11, 2008, page 18, lines 12-14) – Examiner did not respond.

Claim 33 further defines the computing device of claim 32 wherein the memory subsystem comprises a memory array in which **after data is written to the array, further writing to the particular memory location is disabled**, such that the data cannot be overwritten. Claim 33 depends from Claim 32 and is therefore allowable for the same reasons set forth above for the allowance of Claim 32.

Gray, on the other hand, includes both ROM 64 and RAM 66 in its memory module 62. While it may not be possible to write to ROM 64 it would be possible to write to RAM 66.

Claim 34 further defines the computing device of claim 33 further including **at least one of a read only memory (ROM) coupled to the memory array and a random access memory (RAM) coupled to the memory array**. Claim 34 depends from Claim 33 and is therefore allowable for the same reasons set forth above for the allowance of Claim 33. Moreover, in Gray, ROM 64 and RAM 66 are the memory array in verification unit 20 – they are not "coupled to a memory array".

Claim 35 further defines the computing device of claim 33 wherein some portions of the memory array are externally accessible but not modifiable. Claim 35 depends from Claim 33 and is therefore allowable for the same reasons set forth above for the allowance of Claim 33.

Claim 36 further defines the computing device of claim 33 wherein **some portions of the memory array <u>are not externally accessible and are not modifiable</u>**. Claim 36 depends from Claim 33 and is therefore allowable for the same reasons set forth above for the allowance of Claim 33. Examiner points out that Gray teaches that memory can be password protected (Col. 9, lines 21-28)(Office Action dated November 1, 2007, page 8, lines 5-7). But Appellants respond that Examiner's above determination is an admission that someone with the password WOULD HAVE ACCESS to the memory – thus Gray fails to teach or suggest, "wherein **some portions of the memory array <u>are not externally accessible and are not modifiable</u>**", as required by Claim 36. Accordingly, the rejection is improper and must be reversed.

Claim 37 further defines the computing device of claim 33 wherein an encryption key is **stored in the memory array**. Claim 37 depends from Claim 33 and is therefore allowable for the same reasons set forth above for the allowance of Claim 33. Moreover, the encryption key in stored in memory on card 34. When the encryption key is read into memory module 62, it is read into RAM 66. Thus, when the encryption key is the data being read into the memory module, it can not be equated to **a memory array in which after data is written to the array, further writing to the particular memory location is disabled, such that the data cannot be overwritten**, as required by Claim 16, the claim upon which Claim 20 depends.

Claim 38 further defines the computing device of claim 37 wherein the **encryption key is generated by a random number generator internal to the processing system**. Claim 38 depends from Claim 37 and is therefore allowable for the same reasons set forth above for the allowance of Claim 37. Moreover, the extent Gray's verification unit does generates something, it generates "session keys" that are sent to the PACS residing the CPU 40 for using in preparing

classified documents and files (Col. 12, lines 8-10). Verification unit 20 may "manage" cipher keys that protect other keys (Col. 12, lines 6-7), but it does not "generate" the encryption keys. Encryption keys are transferred from cards 34 and then stored in RAM 66 for comparison to the keys being input via keyboard 16 – NOT "**generated by a random number generator internal to the processing system**", as required by Claim 38.

Claim 40 further defines the computing device of claim 33, further including at least one processor coupled to the memory subsystem. Claim 40 depends from Claim 33 and is therefore allowable for the same reasons set forth above for the allowance of Claim 33.

Claim 41 further defines the computing device of claim 31, further including a non-volatile memory system coupled to the baseband processing system wherein the non-volatile memory system is external to the processing system but internal to the computing device. Claim 41 depends from Claim 31 and is therefore allowable for the same reasons set forth above for the allowance of Claim 31. In addition to the above, if Examiner takes the position that Gray's memory module 62 and processor 60 are the "processing system", then Gray further fails to teach or suggest, "a non-volatile memory system coupled to the processing system wherein **the non-volatile memory system is external to the processing system but internal to the computing device**".

Claim 43 further defines the computing device of claim 34, further comprising **at least one of the following stored in the array: a test ID; a manufacturer's public key; a die identification number**. Claim 43 depends from Claim 34 and is therefore allowable for the same reasons set forth above for the allowance of Claim 34. Moreover, in Gray, upon receipt of the password from keyboard 16, verification unit 20 encrypts and temporarily stores the password in RAM 66 (Col. 6, lines 55-57). It then proceeds to read the encrypted password stored into the in the card 34 through card reader 68, and compares the encrypted password received from the card 34 with the encrypted password stored in RAM 66 (Col. 6, lines 57-60).

Gray, however, fails to further teach or suggest, "**at least one of the following stored in the array: a test ID; a manufacturer's public key; a die identification number**", as further required by Claim 43.

Claim 44 further defines the computing device of claim 35 wherein the read only memory (ROM) further comprises at least one of the following: a program for determining whether boot system firmware is available for uploading at power-up; a program for checking authenticity and integrity of the system boot firmware; a program for preventing alternation of specific data associated with the computing device; a program for preventing alteration or swapping of firmware; cryptographic software. Claim 44 depends from Claim 35 and is therefore allowable for the same reasons set forth above for the allowance of Claim 35.

Claim 45 further defines the computing device of claim 41, wherein the non-volatile memory system includes at least one of the following: firmware; application software; data files; a manufacturer's certificate; a platform certificate. Claim 45 depends from Claim 41 and is therefore allowable for the same reasons set forth above for the allowance of Claim 41.

2) Claims 2, 3, 8, 9, 29 and 46 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Gray and Lohstroh et al, US patent 5,768,373. Appellants respectfully traverse this rejection as set forth below.

Independent Claim 1, the claim from which Claims 2, 3 and 29 depend, requires and positively recites, a method of **securing access to resources** **in a computing device**, comprising the steps of: "storing an encrypted access code **in a memory location** **within the computing device**", "receiving a password **to access the resources**", "encrypting the password to produce a encrypted password", "comparing the encrypted password to the encrypted access code", and "**allowing access to the resources** if the encrypted access code matches the encrypted

password".

Independent Claim 7, as amended, the claim from which Claims 8, 9 and 46 depend, requires and positively recites, a **computing device comprising**: "a processing system", "a **memory coupled to the processing system for storing an encrypted access code**", "input circuitry coupled to the processing system for receiving a password to **access resources**, wherein the processing circuitry: encrypts the password to produce a encrypted password; compares the encrypted password to the encrypted access code; and allows access to the resources if the encrypted access code matches the encrypted password".

Claim 2 further defines the method of claim 1 wherein the step of storing an encrypted access code comprises the step of **storing a hashed access code**. Even if, arguedo, Lohstroh teaches "hashing for use in encryption", Lohstroh fails to teach or suggest the previously deficiencies of Gray with respect to Claim 1. As such, any combination of Gray and Lohstroh fails to teach or suggest all of the limitations of Claim 2.

Claim 3 further defines the method of claim 2 wherein the step of encrypting a password comprises the step of **hashing a password**. Even if, arguedo, Lohstroh teaches "hashing for use in encryption", Lohstroh fails to teach or suggest the previously deficiencies of Gray with respect to Claim 2. As such, any combination of Gray and Lohstroh fails to teach or suggest all of the limitations of Claim 3.

Claim 8 further defines the computing device of claim 7 wherein the encrypted access code comprises **a hashed access code**. Even if, arguedo, Lohstroh teaches "hashing for use in encryption", Lohstroh fails to teach or suggest the previously deficiencies of Gray with respect to Claim 7. As such, any combination of Gray and Lohstroh fails to teach or suggest all of the limitations of Claim 8.

Claim 9 further defines the computing device of claim 8 wherein the encrypted password comprises **a hashed password**. Even if, arguedo, Lohstroh teaches "hashing for use in encryption", Lohstroh fails to teach or suggest the previously deficiencies of Gray with respect to Claim 8. As such, any combination of Gray and Lohstroh fails to teach or suggest all of the limitations of Claim 8.

Claim 29 further defines the method of claim 1 wherein the encrypted password **is of a different length than the received password**. Even if, arguedo, Lohstroh teaches "using hashing to reduce a large block of data to a smaller block of data", as suggested by Examiner, Lohstroh fails to teach or suggest the previously deficiencies of Gray with respect to Claim 1. As such, any combination of Gray and Lohstroh fails to teach or suggest all of the limitations of Claim 29.

Claim 46 further defines the computing device of claim 7 wherein the encrypted password **is of a different length than the received password**. Even if, arguedo, Lohstroh teaches "using hashing to reduce a large block of data to a smaller block of data", as suggested by Examiner, Lohstroh fails to teach or suggest the previously deficiencies of Gray with respect to Claim 7. As such, any combination of Gray and Lohstroh fails to teach or suggest all of the limitations of Claim 46

In proceedings before the Patent and Trademark Office, "the Examiner bears the burden of establishing a prima facie case of obviousness based upon the prior art". *In re Fritch*, 23 USPQ2d 1780, 1783 (Fed. Cir. 1992) (citing *In re Piasecki*, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787-88 (Fed. Cir. 1984). "The Examiner can satisfy this burden **only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references**", *In re Fritch*, 23 USPQ2d 1780, 1783 (Fed. Cir. 1992)(citing *In re Fine*, 837 F.2d

1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988)(citing *In re Lalu*, 747 F.2d 703, 705, 223 USPQ 1257, 1258 (Fed. Cir. 1988)).

Moreover, **it is impermissible to use the claimed invention as an instruction manual or "template" to piece together the teachings of the prior art so that the claimed invention is rendered obvious**. *In re Gorman*, 933 F.2d 982, 987, 18 USPQ2d 1885, 1888 (Fed.Cir.1991). See also *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1138, 227 USPQ 543, 547 (Fed.Cir.1985).

Furthermore, "all words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). Accordingly, Claims 2, 3, 8, 9, 27 and 46 are patentable under 35 U.S.C. § 103(a) over Gray in view of Lohstroh.

3) Claims 14, 25, 31, 32 and 42 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Gray in view of Reddy, US patent 6,824,051. Appellants respectfully traverse this rejection as set forth below.

Independent Claim 1, the claim from which Claims 2, 3 and 29 depend, requires and positively recites, a method of **securing access to resources in a computing device**, comprising the steps of: "storing an encrypted access code **in a memory location within the computing device**", "receiving a password **to access the resources**", "encrypting the password to produce a encrypted password", "comparing the encrypted password to the encrypted access code", and "**allowing access to the resources** if the encrypted access code matches the encrypted password".

Independent Claim 7, as amended, the claim from which Claims 8, 9 and 46 depend, requires and positively recites, a **computing device comprising**: "a processing system", "a **memory coupled to the processing system for storing an encrypted access code**", "input circuitry coupled to the processing system for receiving a password to **access resources**, wherein the processing circuitry: encrypts the password to produce a encrypted password; compares the encrypted password to the encrypted access code; and allows access to the resources if the encrypted access code matches the encrypted password".

Claim 14 further defines the method of claim 13, wherein the processing system is **a baseband processing system**. Even if, arguedo, Reddy teaches "a PDA embodiment", Reddy fails to teach or suggest the previously deficiencies of Gray with respect to Claim 1 (claim from which Claim 14 ultimately depends). As such, any combination of Gray and Reddy fails to teach or suggest all of the limitations of Claim 14. Further, since there is no teaching or suggestion in Reddy for computers requiring RF communication, if would not be obvious to incorporate a baseband processing system into the device of Gray. Examiner's determination is supposition not supported by fact. The rejection is improper and must be reversed.

Claim 25 further defines the method of claim 24, further including **a radio frequency (RF) system** coupled to the processing system. Even if, arguendo, Reddy teaches "a PDA embodiment", Reddy fails to teach or suggest the previously deficiencies of Gray with respect to Claim 1 (claim from which Claim 25 ultimately depends). As such, any combination of Gray and Reddy fails to teach or suggest all of the limitations of Claim 25. Further, since there is no teaching or suggestion in Reddy for computers requiring RF communication, if would not be obvious to incorporate a radio frequency system to the processing system in the device of Gray. Examiner's determination is supposition not supported by fact. The rejection is improper and must be reversed.

Claim 31 further defines the computing device of claim 30 wherein the processing system, the memory and the input/output comprise **a baseband processing system**. Even if, arguendo, Reddy teaches "a PDA embodiment", Reddy fails to teach or suggest the previously deficiencies of Gray with respect to Claim 7 (claim from which Claim 31 ultimately depends). As such, any combination of Gray and Reddy fails to teach or suggest all of the limitations of Claim 31. Further, since there is no teaching or suggestion in Reddy for computers requiring RF communication, if would not be obvious to incorporate a baseband processing system into the device of Gray. Examiner's determination is supposition not supported by fact. The rejection is improper and must be reversed.

Claim 32 further defines the computing device of claim 31 wherein the memory location is in a memory subsystem **within the baseband processing system**. Even if, arguendo, Reddy teaches "a PDA embodiment", Reddy fails to teach or suggest the previously deficiencies of Gray with respect to Claim 7 (claim from which Claim 32 ultimately depends). As such, any combination of Gray and Reddy fails to teach or suggest all of the limitations of Claim 32. Further, since there is no teaching or suggestion in Reddy for computers requiring RF communication, if would not be obvious to incorporate a radio frequency system to the processing system in the device of Gray. Examiner's determination is supposition not supported by fact. The rejection is improper and must be reversed.

Claim 42 further defines the computing device of claim 41, further including **a radio frequency (RF) system coupled to the baseband processing system**. Even if, arguendo, Reddy teaches "a PDA embodiment", Reddy fails to teach or suggest the previously deficiencies of Gray with respect to Claim 7 (claim from which Claim 42 ultimately depends). As such, any combination of Gray and Reddy fails to teach or suggest all of the limitations of Claim 42. Further, since there is no teaching or suggestion in Reddy for computers requiring RF communication, if would not be obvious to incorporate a radio frequency system to the

processing system in the device of Gray. Examiner's determination is supposition not supported by fact. The rejection is improper and must be reversed.

In proceedings before the Patent and Trademark Office, "the Examiner bears the burden of establishing a prima facie case of obviousness based upon the prior art". *In re Fritch*, 23 USPQ2d 1780, 1783 (Fed. Cir. 1992) (citing *In re Piasecki*, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787-88 (Fed. Cir. 1984). "The Examiner can satisfy this burden **only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references**", *In re Fritch*, 23 USPQ2d 1780, 1783 (Fed. Cir. 1992)(citing *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988)(citing *In re Lalu*, 747 F.2d 703, 705, 223 USPQ 1257, 1258 (Fed. Cir. 1988)).

Moreover, **it is impermissible to use the claimed invention as an instruction manual or "template" to piece together the teachings of the prior art so that the claimed invention is rendered obvious.** *In re Gorman*, 933 F.2d 982, 987, 18 USPQ2d 1885, 1888 (Fed.Cir.1991). See also *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1138, 227 USPQ 543, 547 (Fed.Cir.1985).

Furthermore, "all words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). Accordingly, Claims 14, 25, 31, 32 and 42 are patentable under 35 U.S.C. § 103(a) over Gray in view of Reddy.

4) Claims 22 and 39 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Gray in view of Debry, US patent 6,341,521. Appellants respectfully traverse this rejection as set forth below.

Independent Claim 1, the claim from which Claim 22 depends, requires and positively recites, a method of **securing access to resources in a computing device**, comprising the steps of: "storing an encrypted access code **in a memory location within the computing device**", "receiving a password **to access the resources**", "encrypting the password to produce a encrypted password", "comparing the encrypted password to the encrypted access code", and "**allowing access to the resources** if the encrypted access code matches the encrypted password".

Independent Claim 7, as amended, the claim from which Claim 39 depends, requires and positively recites, a **computing device comprising**: "a processing system", "a **memory coupled to the processing system for storing an encrypted access code**", "input circuitry coupled to the processing system for receiving a password to **access resources**, wherein the processing circuitry: encrypts the password to produce a encrypted password; compares the encrypted password to the encrypted access code; and allows access to the resources if the encrypted access code matches the encrypted password".

Claim 22 further defines the method of claim 21 wherein the encryption key is generated **at the time of production of the processing system**. Even if, arguendo, Debry teaches "a device that the encryption key is generated and stored at the time of manufacture", as suggested by Examiner, Debry fails to teach or suggest the previously deficiencies of Gray with respect to Claim 1 (claim from which Claim 22 ultimately depends). As such, any combination of Gray and Debry fails to teach or suggest all of the limitations of Claim 22. Examiner's determination is supposition not supported by fact. The rejection is improper and must be reversed.

Claim 39 further defines the computing device of claim 38 wherein the encryption key is generated **at the time of production of the processing system**. Even if, arguendo, Debry teaches "a device that the encryption key is generated and stored at the time of manufacture", as

suggested by Examiner, Debry fails to teach or suggest the previously deficiencies of Gray with respect to Claim 7 (claim from which Claim 39 ultimately depends). As such, any combination of Gray and Debry fails to teach or suggest all of the limitations of Claim 39. Examiner's determination is supposition not supported by fact. The rejection is improper and must be reversed.

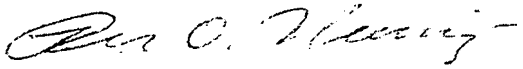
In proceedings before the Patent and Trademark Office, "the Examiner bears the burden of establishing a prima facie case of obviousness based upon the prior art". *In re Fritch*, 23 USPQ2d 1780, 1783 (Fed. Cir. 1992) (citing *In re Piasecki*, 745 F.2d 1468, 1471-72, 223 USPQ 785, 787-88 (Fed. Cir. 1984). "The Examiner can satisfy this burden **only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references**", *In re Fritch*, 23 USPQ2d 1780, 1783 (Fed. Cir. 1992)(citing *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988)(citing *In re Lalu*, 747 F.2d 703, 705, 223 USPQ 1257, 1258 (Fed. Cir. 1988)).

Moreover, **it is impermissible to use the claimed invention as an instruction manual or "template" to piece together the teachings of the prior art so that the claimed invention is rendered obvious.** *In re Gorman*, 933 F.2d 982, 987, 18 USPQ2d 1885, 1888 (Fed.Cir.1991). See also *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1138, 227 USPQ 543, 547 (Fed.Cir.1985).

Furthermore, "all words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). Accordingly, Claims 22 and 39 are patentable under 35 U.S.C. § 103(a) over Gray in view of Debry.

For the above reasons, favorable consideration of the appeal of the Final Rejection in the above-referenced application, and its reversal, are respectfully requested.

Respectfully submitted,



/Ronald O. Neerings/
Reg. No. 34,227
Attorney for Appellants

TEXAS INSTRUMENTS INCORPORATED
P.O. BOX 655474, M/S 3999
Dallas, Texas 75265
Phone: 972/917-5299
Fax: 972/917-4418

CLAIMS APPENDIX

CLAIMS ON APPEAL:

1. A method of securing access to resources in a computing device, comprising the steps of:

storing an encrypted access code in a memory location within the computing device;

receiving a password to access the resources;

encrypting the password to produce a encrypted password;

comparing the encrypted password to the encrypted access code;

allowing access to the resources if the encrypted access code matches the encrypted password.

2. The method of claim 1 wherein the step of storing an encrypted access code comprises the step of storing a hashed access code.

3. The method of claim 2 wherein the step of encrypting a password comprises the step of hashing a password.

4. The method of claim 1 wherein the encrypted access code is stored in a memory that cannot be externally modified.

5. The method of claim 1 wherein the step of allowing access comprises the step of allowing access to testing resources if the encrypted access code matches the encrypted password.

6. The method of claim 1 wherein the step of allowing access comprises the step of allowing access to change system parameters if the encrypted access code matches the encrypted password.

7. A computing device comprising:

a processing system;

a memory coupled to the processing system for storing an encrypted access code;

input circuitry coupled to the processing system for receiving a password to access resources;

wherein the processing circuitry:

encrypts the password to produce a encrypted password;

compares the encrypted password to the encrypted access code;

allows access to the resources if the encrypted access code matches the encrypted password.

8. The computing device of claim 7 wherein the encrypted access code comprises a hashed access code.

9. The computing device of claim 8 wherein the encrypted password comprises a hashed password.

10. The computing device of claim 7 wherein the encrypted access code is stored in a memory that cannot be externally modified.

11. The computing device of claim 7 wherein the processing system allows access to testing resources if the encrypted access code matches the encrypted password.

12. The computing device of claim 7 wherein the processing system allows access to system parameters if the encrypted access code matches the encrypted password.

13. The method of claim 1 wherein the memory location is within a processing system in the computing device.

14. The method of claim 13, wherein the processing system is a baseband processing system.

15. The method of claim 13 wherein the memory location is in a memory subsystem within the processing system.

16. The method of claim 15 wherein the memory subsystem comprises a memory array in which after data is written to the array, further writing to the particular memory location is disabled, such that the data cannot be overwritten.

17. The method of claim 16 further including at least one of a read only memory (ROM) coupled to the memory array and a random access memory (RAM) coupled to the memory array.

18. The method of claim 16 wherein some portions of the memory array are externally accessible but not modifiable.

19. The method of claim 16 wherein some portions of the memory array are not externally accessible and are not modifiable.

20. The method of claim 16 wherein an encryption key is stored in the memory array.

21. The method of claim 20 wherein the encryption key is generated by a random number generator internal to the processing system.

22. The method of claim 21 wherein the encryption key is generated at the time of production of the processing system.

23. The method of claim 15, further including at least one processor coupled to the memory subsystem.

24. The method of claim 23, further including a non-volatile memory system coupled to the processing system wherein the non-volatile memory system is external to the processing system but internal to the computing device.

25. The method of claim 24, further including a radio frequency (RF) system coupled to the processing system.

26. The method of claim 16, further comprising at least one of the following stored in the array: a test ID; a manufacturer's public key; a die identification number.

27. The method of claim 17 wherein the read only memory (ROM) further comprises at least one of the following: a program for determining whether boot system firmware is available for uploading at power-up; a program for checking authenticity and integrity of the system boot firmware; a program for preventing alternation of specific data associated with the computing device; a program for preventing alteration or swapping of firmware; cryptographic software.

28. The method of claim 24, wherein the non-volatile memory system includes at least one of the following: firmware; application software; data files; a manufacturer's certificate; a platform certificate.

29. The method of claim 1 wherein the encrypted password is of a different length than the received password.

30. The computing device of claim 7 wherein the memory is a memory subsystem within the computing device.

31. The computing device of claim 30 wherein the processing system, the memory and the input/output comprise a baseband processing system.

32. The computing device of claim 31 wherein the memory location is in a memory subsystem within the baseband processing system.

33. The computing device of claim 32 wherein the memory subsystem comprises a memory array in which after data is written to the array, further writing to the particular memory location is disabled, such that the data cannot be overwritten.

34. The computing device of claim 33 further including at least one of a read only memory (ROM) coupled to the memory array and a random access memory (RAM) coupled to the memory array.

35. The computing device of claim 33 wherein some portions of the memory array are externally accessible but not modifiable.

36. The computing device of claim 33 wherein some portions of the memory array are not externally accessible and are not modifiable.

37. The computing device of claim 33 wherein an encryption key is stored in the memory array.

38. The computing device of claim 37 wherein the encryption key is generated by a random number generator internal to the processing system.

39. The computing device of claim 38 wherein the encryption key is generated at the time of production of the processing system.

40. The computing device of claim 33, further including at least one processor coupled to the memory subsystem.

41. The computing device of claim 31, further including a non-volatile memory system coupled to the baseband processing system wherein the non-volatile memory system is external to the processing system but internal to the computing device.

42. The computing device of claim 41, further including a radio frequency (RF) system coupled to the baseband processing system.

43. The computing device of claim 34, further comprising at least one of the following stored in the array: a test ID; a manufacturer's public key; a die identification number.

44. The computing device of claim 35 wherein the read only memory (ROM) further comprises at least one of the following: a program for determining whether boot system firmware is available for uploading at power-up; a program for checking authenticity and integrity of the system boot firmware; a program for preventing alternation of specific data associated with the computing device; a program for preventing alteration or swapping of firmware; cryptographic software.

45. The computing device of claim 41, wherein the non-volatile memory system includes at least one of the following: firmware; application software; data files; a manufacturer's certificate; a platform certificate.

46. The computing device of claim 7 wherein the encrypted password is of a different length than the received password.

RELATED PROCEEDINGS APPENDIX

Appellant is not aware of pending appeals in any related applications.

EVIDENCE APPENDIX

No documents are being submitted with the Appeal Brief.